SYSTEM AND METHOD FOR AUTHENTICATING PEER COMPONENTS

Publication number:	EP1047992
Publication date:	2000-11-02
Inventor:	BENSON GREG (US); FRANKLIN MARTIN (US); KNAUFT CHRISTOPHER L (US)
Applicant:	MEDIADNA INC (US)
Classification:	
- international:	***G06F21/22; G06F1/00; G06F21/00; G06F21/20;*** **G06F21/22; G06F1/00; G06F21/00; G06F21/20;** (IPC1-7): G06F11/00
- european:	G06F1/00R4T; G06F21/00N3V4T; G06F21/00N9C
Application number:	EP19990903135 19990115
Priority number(s):	WO1999US00968 19990115; US19980071737P 19980116

Also published as:

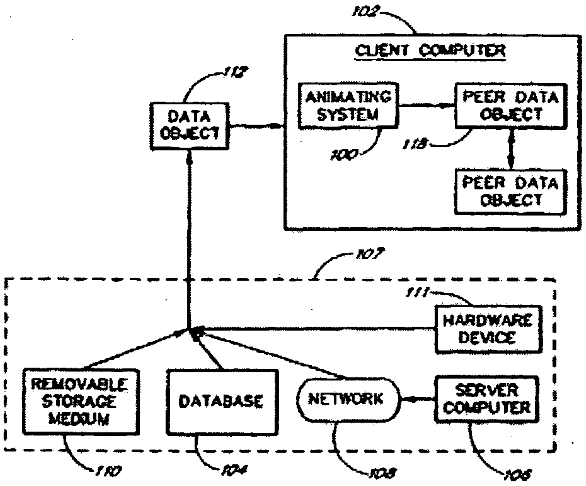
- WO9936854 (A1)
- EP1047992 (A0)
- CA2315212 (A1)
- EP1047992 (B1)
- ES2175936T (T3)

more >>

Report a data error here

Abstract not available for EP1047992
Abstract of corresponding document: **WO9936854**

A system and method for controlling the usage of data objects in component object systems. According to the invention, each data object (112) includes a peer list that defines one or more peer data objects (118) that are required by the data object (112). Upon receipt of a data object (112), the system verifies the integrity of the data object (112). Further, the system identifies the integrity of the peer data objects (118). If the system cannot find the peer data objects (118), or the system cannot authenticate the peer data objects (118), the system may optionally retrieve a peer data object that can be authenticated from a data object depository. In addition to validating the integrity of the data object (112), the system verifies that the data object (112) is authorized to communicate with each of the peer data objects (118). Further, the system verifies that the peer data objects (118) are authorized to communicate with the data object (112).



Data supplied from the ***esp@cenet*** database - Worldwide

Secure mutual network authentication protocol

Publication number: EP1069726
Publication date: 2001-01-17
Inventor: MACKENZIE PHILIP DOUGLAS (US); SWAMINATHAN RAM (US)
Applicant: LUCENT TECHNOLOGIES INC (US)
Classification:
- international: *G06F21/20; H04L9/08; H04L9/32;* **G06F21/20; H04L9/08; H04L9/32;** (IPC1-7): H04L9/32
- european: H04L9/08D2; H04L9/32
Application number: EP20000305566 20000703
Priority number(s): US19990353468 19990713

Also published as:
US6757825 (B1)
JP2001060947 (A)
EP1069726 (A3)
CA2313557 (A1)

Cited documents:
WO9920020
XP002267460

Report a data error here

Abstract of **EP1069726**

A password-only mutual network authentication protocol and key exchange protocol using a public key encryption scheme in which a server generates a public key / secret key pair and transmits the public key to a client. The client determines whether the public key was chosen in an acceptable manner, and if so, continues with the protocol. Otherwise, the client rejects authentication. If the protocol is continued, in one embodiment the client generates a parameter p as a function of the public key and a password (or, in an alternate embodiment, as a function of the public key and a function of a password). If the public key space mapping function FPK applied to p, FPK(p), is an element of the public key message space, then the protocol continues. If FPK(p) is not an element of the public key message space, then the client determines to reject authentication, but continues with the protocol so that the server does not gain any information about the password. If the client determines to reject authentication, it will terminate the protocol at a later step at which time the termination of the protocol cannot leak any sensitive information. If both the client and the server accept authentication, then session keys are generated for subsequent secure communication between the client and server. Specific embodiments are disclosed in which RSA is used as the public key encryption scheme.

Data supplied from the ***esp@cenet*** database - Worldwide